PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-007214

(43)Date of publication of application : 11.01.2002

(51)Int.Cl. G06F 12/14
G06F 1/00

(21)Application number : 2000-192757

(22)Date of filing : 27.06.2000

(71)Applicant : TOSHIBA CORP

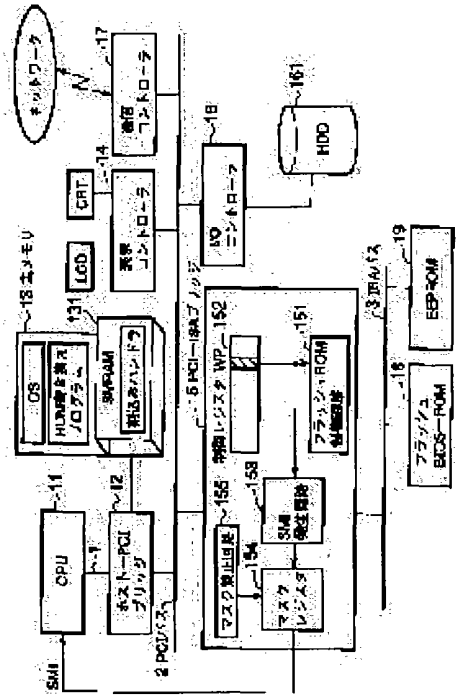
(72)Inventor : MAEDA MAYUMI

(54) INFORMATION PROCESSOR AND REWRITE CONTROL METHOD OF NONVOLATILE STORAGE DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve security level by stopping a nonvolatile storage device from being rewritten in unauthorized manner by software.

SOLUTION: A ROM rewriting program performs access for rewriting a write protect bit WP in a control register 152 to '1' in a series of ROM rewrite processes and releases the write protect of a flash BIOS-ROM 18. At this time, an SMI-generating circuit 153 issues an SMI signal to a CPU 11. In response to this SMI signal, an interrupt handler is actuated. The interrupt handler authenticates whether the access by the ROM rewriting program is authorized, and performs access for rewriting the write protect bit WP in a control register 152 to '0' and re-sets the write protect of the flash BIOS-ROM 18, and stops the rewriting when deciding that the access is not authorized.



LEGAL STATUS

[Date of request for examination] 27.06.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－7214
（P2002－7214A）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ　５Ｂ０１７
1/00		9/06	６６０Ｊ　５Ｂ０７６

審査請求　有　　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願2000－192757(P2000－192757)

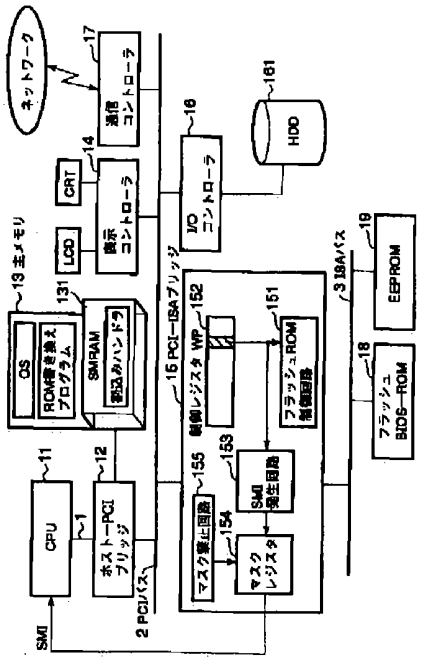
(22)出願日　平成12年６月27日(2000.6.27)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　前田　真弓
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B017 AA02 BA04 BB00 CA12
5B076 FB02

(54)【発明の名称】　情報処理装置および不揮発性記憶装置の書き換え制御方法

(57)【要約】
【課題】ソフトウェアによる不揮発性記憶装置の不正な書き換えを阻止できるようにし、セキュリティーレベルの向上を図る。
【解決手段】ＲＯＭ書き換えプログラムは、一連のＲＯＭ書き換え処理の中で、制御レジスタ１５２内のライトプロテクトビットＷＰを“1”に書き換えるアクセスを実行し、フラッシュＢＩＯＳ－ＲＯＭ１８のライトプロテクトを解除する。このとき、ＳＭＩ発生回路１５３からＣＰＵ１１にＳＭＩ信号が発行される。このＳＭＩ信号に応答して、割り込みハンドラが起動される。割り込みハンドラは、ＲＯＭ書き換えプログラムによるアクセスが正当なものであるか否かの認証を行い、正当なアクセスではないと判定した場合には、書き換えを阻止するために、制御レジスタ１５２内のライトプロテクトビットＷＰを“0”に書き換えるアクセスを実行し、フラッシュＢＩＯＳ－ＲＯＭ１８のライトプロテクトを再設定する。



【特許請求の範囲】
【請求項１】　不揮発性記憶装置の記憶内容を書き換え可能な情報処理装置であって、
ＣＰＵと、
前記不揮発性記憶装置の書き換えに必要な所定のハードウェアに対する、ソフトウェアからのアクセスに応答して、前記ＣＰＵに割り込み信号を発生する割り込み信号発生手段と、
前記割り込み信号発生手段からの割り込み信号の発生を契機に前記ＣＰＵによって起動され、前記ソフトウェアによるアクセスが不当なものである場合、前記不揮発性記憶装置の書き換えを禁止する書き換え制御手段とを具備することを特徴とする情報処理装置。
【請求項２】　前記書き換え制御手段は、
前記ハードウェアに対するアクセスに先立って実行すべき所定の手順が前記ソフトウェアによってすでに実行されているか否かを判別する手段を含み、その判別結果に応じて前記ソフトウェアによるアクセスが不当なものであるか否かを検出することを特徴とする請求項１記載の情報処理装置。
【請求項３】　前記割り込み信号のマスクを禁止するためのマスク禁止手段をさらに具備することを特徴とする請求項１記載の情報処理装置。
【請求項４】　前記不揮発性記憶装置の書き換えを禁止するためのライトプロテクト機能を有し、前記ライトプロテクト機能の設定が解除されている場合、ソフトウェアからのアクセスに応答して前記不揮発性記憶装置の書き換えに必要な動作を実行するアクセス制御手段をさらに具備し、
前記割り込み信号発生手段は、前記アクセス制御手段に対してライトプロテクトを解除するためのアクセスがソフトウェアによって行われたとき、それに応答して前記割り込み信号を発生することを特徴とする請求項１記載の情報処理装置。
【請求項５】　前記書き換え制御手段は、前記ソフトウェアによる前記ライトプロテクトを解除するためのアクセスが不当なものである場合、前記ソフトウェアによる前記不揮発性記憶装置の書き換えを阻害するために前記アクセス制御手段をアクセスして、ライトプロテクトを再設定する手段を含むことを特徴とする請求項４記載の情報処理装置。
【請求項６】　前記書き換え制御手段は、前記ソフトウェアによるアクセスが不当なものである場合、前記ソフトウェアによる前記不揮発性記憶装置の書き換えを阻害するために前記情報処理装置をシャットダウンする手段を含むことを特徴とする請求項１記載の情報処理装置。
【請求項７】　前記不揮発性記憶装置には、前記情報処理装置のハードウェア制御のためのＢＩＯＳプログラムが格納されていることを特徴とする請求項１記載の情報処理装置。
【請求項８】　不揮発性メモリに格納されているＢＩＯＳプログラムをオペレーティングシステムの動作環境下で書き換え可能な情報処理装置であって、
ＣＰＵと、
前記不揮発性メモリの書き換え動作を実行するアクセス制御手段と、
前記オペレーティングシステム上で動作するソフトウェアからの前記アクセス制御手段に対する所定のアクセスに応答して、前記ＣＰＵに割り込み信号を発生する割り込み信号発生手段とを具備し、
前記ＣＰＵは、前記割り込み信号によって割り込み処理を実行し、その割り込み処理の中で、前記ソフトウェアによる前記アクセス制御手段に対するアクセスが不当なものであるか否かを検出し、不当なものである場合、前記不揮発性メモリの書き換えを禁止するための処理を行うことを特徴とする情報処理装置。
【請求項９】　情報処理装置内で使用される不揮発性記憶装置の記憶内容の書き換えを制御するための書き換え制御方法であって、
前記情報処理装置内のＣＰＵによって実行されるソフトウェアが前記不揮発性記憶装置の書き換えに必要な前記情報処理装置内の所定のハードウェアにアクセスしたとき、そのアクセスに応答して前記ＣＰＵに割り込み信号を発生するステップと、
前記割り込み信号の発生を契機に前記ＣＰＵによって起動される割り込み処理の中で、前記ソフトウェアによるアクセスが不当なものであるか否かを検出し、不当なものである場合、前記不揮発性記憶装置の書き換えを禁止するための処理を実行するステップとを具備することを特徴とする書き換え制御方法。
【請求項１０】　前記不揮発性記憶装置には、前記情報処理装置のハードウェア制御のためのＢＩＯＳプログラムが格納されていることを特徴とする請求項９記載の書き換え制御方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はパーソナルコンピュータなどの情報処理装置およびその情報処理装置で使用される不揮発性記憶装置の書き換え制御方法に関する。
【０００２】
【従来の技術】近年、携行が容易でバッテリにより動作可能なノートブックタイプのパーソナルコンピュータ（ＰＣ）が種々開発されている。この種のＰＣに於いては、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）を新しいバージョンにアップグレードするというＢＩＯＳアップデートを行えるようにするために、ＢＩＯＳはフラッシュメモリなどの電気的に書き換え可能な不揮発性メモリに格納されている。
【０００３】ＢＩＯＳの更新は、通常は、更新用の新たなＢＩＯＳファイルおよびＢＩＯＳ更新用システムプロ

グラムを収めたフロッピー（登録商標）ディスク（ＦＤ）をＰＣに装填した状態でＰＣをパワーオンし、ＦＤからＢＩＯＳ更新用システムプログラムを起動することによって行われる。また、最近では、オペレーティングシステムの動作環境下で動作する専用のアプリケーションを実行することによって、ＢＩＯＳの更新を行う方法も考えられている。この方法により、ＦＤからシステムを起動する必要が無くなるので、フロッピーディスクドライブ（ＦＤＤ）が装備されていない、いわゆるＦＤＤレスのＰＣにおいても、容易にＢＩＯＳをアップデートすることが可能となる。

【０００４】ＢＩＯＳ更新のための不揮発性メモリの書き換え手順はＰＣのプラットフォーム毎に個々に規定されるものではあるが、その書き換え手順は基本的には公開されている場合が多い。このため、その書き換え手順を実行するプログラムを作成して実行させることにより、誰でも容易に不揮発性メモリの中身を変更することができる。

【０００５】

【発明が解決しようとする課題】この場合、不揮発性メモリの書き換え手順が正しい限りにおいてはその書き換えを阻止することは困難である。したがって、もし悪意を持つ人がそのような書き換えプログラムを作成してそれをインターネット等を通じてウィルスとして配布すると、そのウィルスを実行したＰＣの不揮発性メモリが不正に書き換えられてしまうという事態を招く危険がある。

【０００６】本発明は上述の事情に鑑みてなされたものであり、ソフトウェアによる不揮発性記憶装置の不正な書き換えを阻止できるようにし、十分にセキュリティーレベルの高い情報処理装置および不揮発性記憶装置の書き換え制御方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】上述の課題を解決するため、本発明は、不揮発性記憶装置の記憶内容を書き換え可能な情報処理装置であって、ＣＰＵと、前記不揮発性記憶装置の書き換えに必要な所定のハードウェアに対する、ソフトウェアからのアクセスに応答して、前記ＣＰＵに割り込み信号を発生する割り込み信号発生手段と、前記割り込み信号発生手段からの割り込み信号の発生を契機に前記ＣＰＵによって起動され、前記ソフトウェアによるアクセスが不当なものである場合、前記不揮発性記憶装置の書き換えを禁止する書き換え制御手段とを具備することを特徴とする。

【０００８】この情報処理装置によれば、不揮発性記憶装置の書き換えに必要な所定のハードウェアに対する、ソフトウェアからのアクセスが発生すると、その時点でＣＰＵに対して割り込み信号が自動的に発行される。そして、ＣＰＵの割り込み処理の中で書き換え制御手段が起動され、正当なアクセスである場合には不揮発性記憶装置の書き換えがその時点で禁止される。このように、不揮発性記憶装置に対する書き換え処理手順が開始されたときに、専用の割り込み信号を発行して書き換え制御手段を起動するという仕組みを用いることにより、不揮発性記憶装置に対する不正な書き換えを阻止できるようになり、セキュリティーレベルの向上を図ることが可能となる。

【０００９】ソフトウェアによるアクセスが不当なものであるか否かの検出方法としては、例えば正当なソフトウェア（例えば、当該情報処理装置の製造メーカから配布されたソフトウェアなど）については書き換え処理とは直接関係しない所定の手順を事前に行うようにしておき、その手順が割り込み信号発生前にすでに行われているかどうかを調べるという方法を利用することができる。これにより、簡単でかつ正確に、ソフトウェアによるアクセスが正当なものであるか不当なものであるかを判定することができる。

【００１０】また、書き換え制御手段の起動が封じられるのを防止するために、割り込み信号のマスクを禁止するためのマスク禁止手段を設けることが好ましい。

【００１１】また、何らかの誤動作等によって不揮発性記憶装置の内容が誤って書き換えられてしまうという事態の発生を防止するために、不揮発性記憶装置の書き換え動作を行うアクセス制御手段にはライトプロテクト機能を設けておくことが好ましい。この場合、ソフトウェアによってライトプロテクト機能が解除されたことを契機に割り込み信号を発生し、そして不正なアクセスである場合には、再度ライトプロテクトの設定を行って不正な書き換えを阻止するという制御を利用することができる。

【００１２】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図１には、本発明の一実施形態に係わるコンピュータシステムの構成が示されている。このコンピュータシステムはバッテリ駆動可能なノートブックタイプのパーソナルコンピュータ（ＰＣ）であり、このＰＣ本体には、図示のように、プロセッサバス１、ＰＣＩバス２、ＩＳＡバス３、ＣＰＵ１１、ホスト－ＰＣＩブリッジ１２、主メモリ１３、表示コントローラ１４、ＰＣＩ－ＩＳＡブリッジ１５、Ｉ／Ｏコントローラ１６、通信コントローラ１７、フラッシュＢＩＯＳ－ＲＯＭ１８、およびＥＥＰＲＯＭ１９などが設けられている。

【００１３】ＣＰＵ１１は本ＰＣ全体の動作を制御するためのものであり、主メモリ１３にロードされるオペレーティングシステム（ＯＳ）及びＲＯＭ書き換えプログラムなどを実行する。ＲＯＭ書き換えプログラムはフラッシュＢＩＯＳ－ＲＯＭ１８を書き換えるためのソフトウェアである。このＲＯＭ書き換えプログラムはＯＳの動作環境下で動作するように構成された一種のアプリケ

ーションプログラムであり、ＢＩＯＳ更新は、ＯＳの動作環境下で実行することができる。

【００１４】ＣＰＵ１１としては、システム管理割り込みＳＭＩ（ＳＭＩ：System Management Interrupt）をサポートするものが利用される。即ち、ＣＰＵ１１はオペレーティングシステムやアプリケーション等を実行するための通常動作モードに加え、システム管理モード（ＳＭＭ：Ｓｙｓｔｅｍ Ｍａｎａｇｅｍｅｎｔｍｏｄｅ）と称されるシステム管理機能を実現するための動作モードを有している。

【００１５】システム管理割込み（ＳＭＩ：System Management Interrupt）がＣＰＵ１１に発行された時、ＣＰＵ１１の動作モードは、通常動作モード（リアルモード、プロテクトモード、または仮想８６モード）から、ＳＭＭにスイッチされる。ＳＭＭでは、ＳＭＲＡＭ１３１上のシステム管理プログラムが実行される。システム管理プログラムは、ＳＭＭ－ＢＩＯＳとしてフラッシュＢＩＯＳ－ＲＯＭ１８に予め記憶されているものであり、システム起動時にフラッシュＢＩＯＳ－ＲＯＭ１８からＳＭＲＡＭ１３１にコピーされる。本実施形態においては、システム管理プログラムの一つとして、不正なＲＯＭ書き換え処理の実行を阻止するための割り込みハンドラが用意されている。この割り込みハンドラは、ＣＰＵ１１がＳＭＭにスイッチしたときに実行される割り込み処理プログラムである。フラッシュＢＩＯＳ－ＲＯＭ１８の書き換えに必要なＰＣＩ－ＩＳＡブリッジ１５内の所定のハードウェアがソフトウェアによってアクセスされると、ＳＭＩがＣＰＵ１１に発行され、これにより割り込みハンドラが起動される。システム起動中においては、ＳＭＲＡＭ１３１にコピーされた割り込みハンドラの内容を書き換えることはできない。

【００１６】ホスト－ＰＣＩブリッジ１２は、ＣＰＵバス１とＰＣＩバス２を双方向で接続するブリッジ装置であり、ここには主メモリ１３をアクセス制御するためのメモリコントロール機能も内蔵されている。表示コントローラ１４は本ＰＣのディスプレイモニタとして使用されるＬＣＤや外部ＣＲＴを制御する。

【００１７】ＰＣＩ－ＩＳＡブリッジ１５は、ＰＣＩバス２とＩＳＡバス３とをつなぐブリッジであり、ＰＣＩバス２のバスマスタとして動作することができる。このＰＣＩ－ＩＳＡブリッジ１５には、フラッシュＢＩＯＳ－ＲＯＭ１８の書き換えに必要な動作を実行するための回路および前述のＳＭＩを発生するための回路などが含まれている。

【００１８】すなわち、ＰＣＩ－ＩＳＡブリッジ１５には、図示のように、フラッシュＲＯＭ制御回路１５１、制御レジスタ１５２、ＳＭＩ発生回路１５３、マスクレジスタ１５４、およびマスク禁止回路１５５などが設けられている。フラッシュＲＯＭ制御回路１５１は、制御レジスタ１５２に設定されるソフトウェアからのコマンドに従ってフラッシュＢＩＯＳ－ＲＯＭ１８のリード／消去／ライト動作を制御する。フラッシュＢＩＯＳ－ＲＯＭ１８の書き換えは、フラッシュＢＩＯＳ－ＲＯＭ１８の内容を一旦消去し、その後、必要なプログラムファイルをフラッシュＢＩＯＳ－ＲＯＭ１８に書き込むことによって行われる。フラッシュＲＯＭ制御回路１５１によるフラッシュＢＩＯＳ－ＲＯＭ１８の消去／ライト動作は、制御レジスタ１５２内のライトプロテクトビットＷＰによって許可又は禁止される。ライトプロテクトビットＷＰ＝“０”にセットすることにより、フラッシュＲＯＭ制御回路１５１によるフラッシュＢＩＯＳ－ＲＯＭ１８の消去およびライト動作の実行は禁止される。ＲＯＭ書き換えプログラムによるＲＯＭ書き換え手順の中には、ライトプロテクトビットＷＰ＝“１”にして、ライトプロテクトを解除する処理が予め含まれている。

【００１９】ＳＭＩ発生回路１５３は、ライトプロテクトビットＷＰが“１”に書き換えられた時、それを要因としてＳＭＩ信号を発生する。マスクレジスタ１５４は、制御レジスタ１５２と同じく、ＣＰＵ１１がリード／ライト可能なレジスタであり、ＳＭＩ信号の発生を許可または禁止するためのマスクデータを保持する。マスク禁止回路１５５はＳＭＩ信号のマスクを禁止するためのものであり、このマスク禁止回路１５５がソフトウェアによってアクティブ状態に設定されると、以降は、ＳＭＩ信号の発生を禁止するためのマスクデータをマスクレジスタ１５４に書き込むことはできなくなる。

【００２０】Ｉ／Ｏコントローラ１６は、２次記憶として用いられるＨＤＤ１６１などのＩＤＥデバイスを制御するためのバスマスタＩＤＥコントローラを内蔵している。バスマスタＩＤＥコントローラは、ＨＤＤ１６１と主メモリ１３との間のデータ転送のためにバスマスタとして動作することができる。また、Ｉ／Ｏコントローラ１６は、ＤＶＤドライブやＣＤ－ＲＯＭドライブを制御することもできる。

【００２１】通信コントローラ１７は例えば公衆網などを介してインターネット上の計算機と通信するためのものであり、モデムやＩＳＤＮカードによって実現されている。ＢＩＯＳ更新を行う場合には、通信コントローラ１７は、バージョンアップされた新たな更新ＢＩＯＳファイルおよびＲＯＭ書き換えプログラムをインターネット上のＷＥＢサーバからダウンロードするために用いられる。ダウンロードされた更新ＢＩＯＳファイルはＨＤＤ１６１に保存される。

【００２２】フラッシュＢＩＯＳ－ＲＯＭ１８は、前述したようにシステムＢＩＯＳを記憶するためのものであり、ソフトウェアによるＢＩＯＳ更新を可能とするために電気的に書き換え可能な不揮発性メモリであるフラッシュメモリ（フラッシュＥＥＰＲＯＭ）によって実現されている。システムＢＩＯＳは、ＰＣのパワーオン時や再起動時に実行されるＰＯＳＴ（ＰｏｗｅｒＯＮ Ｓｅ

ｌｆ　Ｔｅｓｔ）ルーチン、各種Ｉ／Ｏデバイスを制御するためのデバイスドライバ群、システム環境を設定するためのＢＩＯＳセットアップルーチンなどを体系化したものであり、ＰＣ内のハードウェアを直接制御するために用いられる。また、このフラッシュＢＩＯＳ－ＲＯＭ１８には、前述のＳＭＭ－ＢＩＯＳも含まれている。

【００２３】ＥＥＰＲＯＭ１９には例えばパスワード等のセキュリティー管理に必要な情報が記憶されている。このＥＥＰＲＯＭ１９に対するリード／消去／ライト動作の制御もフラッシュＲＯＭ制御回路１５１によって行うことができる。

【００２４】（フラッシュＲＯＭ書き換えに関するセキュリティー）本実施形態のシステムにおいては、フラッシュＲＯＭ書き換えに関するセキュリティー機能として、以下の５つの機能が実装されている。

【００２５】（１）　不適切なフラッシュＢＩＯＳ－ＲＯＭ１８の書き換えに対しては、その書き換え手順の中の特定の処理により専用の割り込み（ＳＭＩ）を発生させる仕組みを使い、割り込みハンドラの中で、フラッシュＲＯＭ書き換えを手順に従って実行してもフラッシュＲＯＭ書き換えが失敗するように書き換え処理を阻止する機能

（２）　フラッシュＲＯＭ書き換え手順の中の特定の処理により発生する専用の割り込み（ＳＭＩ）は、フラッシュＲＯＭ書き換えを行おうとしている時点ではマスクできないようにする機能

（３）　フラッシュＲＯＭ書き換えを行おうとしている時点では、割り込みハンドラ自体を書き換えできないようにする機能

（４）　割り込みハンドラの中で実行するフラッシュＲＯＭ書き換え阻害処理は、それに悪意の書き換え者が気が付いて排除しようとしても排除できないようにする機能

（５）　適正なフラッシュＲＯＭ書き換えに対しては、割り込みハンドラの中で、フラッシュＲＯＭ書き換え阻害処理は行わず、正しくフラッシュＢＩＯＳ－ＲＯＭ１８の書き換えを実行できるようにする機能

（フラッシュＲＯＭ書き換え制御処理＃１）次に、図２のフローチャートを参照して、フラッシュＲＯＭ書き換え制御処理の手順について具体的に説明する。

【００２６】ＲＯＭ書き換えプログラムは、一連のＲＯＭ書き換え処理の中で、制御レジスタ１５２内のライトプロテクトビットＷＰを“１”に書き換えるハードウェアアクセスを実行し、フラッシュＢＩＯＳ－ＲＯＭ１８のライトプロテクトを解除する（ステップＳ１０１）。このとき、ＳＭＩ発生回路１５３からＣＰＵ１１にＳＭＩ信号が発行される。このＳＭＩ信号に応答して、実行中のＲＯＭ書き換えプログラムが中断され、割り込みハンドラに制御が移される。

【００２７】割り込みハンドラは、ＲＯＭ書き換えプログラムによるアクセスが正当なものであるか否かの認証を行い（ステップＳ２０１）、正当な書き換えのためのアクセスであるかどうかを判定する（ステップＳ２０２）。この認証は、例えば、割り込まれたプログラムのプロセス名をチェックして当該ＰＣの製造メーカから配布されたソフトウェアであるか否かを判定したり、あるいは正当なソフトウェアについては書き換え処理とは直接関係しない所定の手順をライトプロテクト解除前に事前に行うようにしておき、その手順がＳＭＩ発生前にすでに行われているかどうかを調べる、ことなどによって行うことができる。

【００２８】ＲＯＭ書き換えのための正当なアクセスであると判定された場合には、割り込みハンドラは、ＳＭＭからの復帰命令（ＲＳＭ）を実行して、ＲＯＭ書き換えプログラムに即座に制御を戻す。ＲＯＭ書き換えプログラムは、フラッシュＲＯＭ制御回路１５１にコマンドを発行し、フラッシュＢＩＯＳ－ＲＯＭ１８の内容を書き換えるための処理（フラッシュＢＩＯＳ－ＲＯＭ１８の消去、書き込み）を実行する（ステップＳ１０２）。これにより、フラッシュＢＩＯＳ－ＲＯＭ１８の内容は正常に更新される。

【００２９】一方、ＲＯＭ書き換えのための正当なアクセスではないと判定された場合には、割り込みハンドラは、制御レジスタ１５２内のライトプロテクトビットＷＰを“０”に書き換えるアクセスを実行し、フラッシュＢＩＯＳ－ＲＯＭ１８のライトプロテクトを再設定する（ステップＳ２０３）。この後、割り込みハンドラは、ＳＭＭからの復帰命令（ＲＳＭ）を実行して、ＲＯＭ書き換えプログラムに制御を戻す。ＲＯＭ書き換えプログラムは、フラッシュＢＩＯＳ－ＲＯＭ１８の内容を書き換えるための処理（フラッシュＢＩＯＳ－ＲＯＭ１８の消去、書き込み）を実行するが（ステップＳ１０２）、ライトプロテクトがなされているので、フラッシュＢＩＯＳ－ＲＯＭ１８の内容を書き換えることはできない。つまり、不正なＲＯＭ書き換えプログラムは、フラッシュＲＯＭ書き換えのための正しい処理を順次行っているにも関わらず、専用の割り込み発生とそれによる割り込みハンドラの処理により、狙い通りにフラッシュＲＯＭ書き換えを完遂することができない。

【００３０】もしＲＯＭ書き換えプログラムがライトプロテクトを再び解除したとしても、その場合には、再び割り込みハンドラによってライトプロテクトが再設定されるので、ＲＯＭ書き換えは失敗する。

【００３１】なお、ＲＯＭ書き換えのための正当なアクセスではないと判定された場合、ライトプロテクトを再設定するだけでなく、不正な書き換えプログラムが実行されている旨の警告メッセージをディスプレイモニタに画面表示して、使用者に注意を促すようにしても良い。

【００３２】（フラッシュＲＯＭ書き換え制御処理＃２）次に、図３のフローチャートを参照して、フラッシ

ュROM書き換え制御処理の第２の手順について説明する。ここでは、予め決められた特定のレジスタに対するライトアクセスが行われているか否かによってプログラム認証が行われる。

【００３３】正当なROM書き換えプログラムは、ステップＳ１０１のライトプロテクト解除処理を行う前に、予め決められた認証用のレジスタ内の所定ビット（認証フラグ）を“1”に設定する（ステップＳ１１１）。この認証用レジスタは本ＰＣ固有のスペシャルレジスタであり、そのＩ／Ｏアドレスおよびアクセス手順は秘密化されている。不正なROM書き換えプログラムは、認証フラグを“1”に設定せずに、ステップＳ１０１のライトプロテクト解除処理を行う。

【００３４】ライトプロテクトが解除されたとき、ＳＭＩ発生回路１５３からＣＰＵ１１にＳＭＩ信号が発行される。このＳＭＩ信号に応答して、ROM書き換えプログラムから割り込みハンドラに制御が移される。割り込みハンドラは、認証フラグをチェックすることによって、ROM書き換えプログラムによるアクセスが正当なものであるか否かの認証を行い（ステップＳ２０１）、正当なアクセスであるかどうかを判定する（ステップＳ２０２）。

【００３５】認証フラグが“1”に設定されていれば、ROM書き換えのための正当なアクセスであると判定される。割り込みハンドラは、ＳＭＭからの復帰命令（ＲＳＭ）を実行して、ROM書き換えプログラムに制御を戻す。ROM書き換えプログラムは、フラッシュＢＩＯＳ－ROM１８の内容を書き換えるための処理（フラッシュＢＩＯＳ－ROM１８の消去、書き込み）を実行する（ステップＳ１０２）。これにより、フラッシュＢＩＯＳ－ROM１８の内容は正常に更新される。

【００３６】一方、認証フラグが“0”であれば、ROM書き換えのための不正アクセスであると判定される。この場合、割り込みハンドラは、制御レジスタ１５２内のライトプロテクトビットWPを“0”に書き換えるアクセスを実行し、フラッシュＢＩＯＳ－ROM１８のライトプロテクトを再設定する（ステップＳ２０３）。この後、割り込みハンドラは、ＳＭＭからの復帰命令（ＲＳＭ）を実行して、ROM書き換えプログラムに制御を戻す。ROM書き換えプログラムは、フラッシュＢＩＯＳ－ROM１８の内容を書き換えるための処理（フラッシュＢＩＯＳ－ROM１８の消去、書き込み）を実行するが（ステップＳ１０２）、ライトプロテクトがなされているので、フラッシュＢＩＯＳ－ROM１８の内容を書き換えることはできない。

【００３７】（フラッシュROM書き換え制御処理＃３）次に、図４のフローチャートを参照して、フラッシュROM書き換え制御処理の第３の手順について説明する。ここでは、ライトプロテクトの再設定によって不正なフラッシュROM書き換えを阻止するのではなく、システムをシャットダウンすることによって阻止するという手法を用いる。

【００３８】即ち、ライトプロテクトの解除によって起動される割り込みハンドラは、図３と同様の手法でROM書き換えプログラムによるアクセスが正当なものであるか否かの認証を行い（ステップＳ２０１）、正当なアクセスであるかどうかを判定する（ステップＳ２０２）。ROM書き換えのための正当なアクセスであると判定された場合は、割り込みハンドラは、ＳＭＭからの復帰命令（ＲＳＭ）を実行するが、ROM書き換えのための不正アクセスであると判定された場合には、その時点でシステム電源を強制的にオフさせることなどによってシステムをシャットダウンする（ステップＳ２０３）。これにより、もはや不正なフラッシュROM書き換えは実行できなくなる。

【００３９】なお、システムをシャットダウンする前にユーザに警告を発して、ライトプロテクトのみを行うか、安全性確保のためにシャットダウンを行うかをユーザに選択させるようにしても良い。

【００４０】（ＳＭＩマスク禁止機能）次に、ＳＭＩのマスク禁止を行うための機能について説明する。上述のように、本実施形態のセキュリティー機能は、ＳＭＩを用いて実現されている。このため、ＳＭＩがマスクされるという妨害を受けると、セキュリティー機能が正常に働かなくなる。これを避けるため、システムＢＩＯＳのＰＯＳＴルーチンは、図５に示すように、ＰＯＳＴ処理の中でマスク禁止回路１５５を制御して、ＳＭＩのマスクを禁止する。

【００４１】（ＳＭＩ発生の他の例）ＳＭＩの発生タイミングは、ライトプロテクト解除時ではなく、図６に示すように、例えばライトプロテクト解除後に行われるフラッシュROM制御回路１５１に対する最初の段階のＩ／Ｏアクセス時であってもよい。すなわち、フラッシュROM制御回路１５１に実際の消去動作を実行させるためにはソフトウェアによって制御レジスタ等に対する何らかのＩ／Ｏアクセスが逐次実行されることになるので、消去動作が実行される前の所定のＩ／Ｏアクセスをトリガに例えばＩ／ＯトラップＳＭＩを発生し、これによって割り込みハンドラを起動させることもできる。

【００４２】（割り込みハンドラの機能拡張）以上、不正なフラッシュROM書き換え処理を阻止するための制御処理について説明したが、本実施形態の仕組みは、フラッシュＢＩＯＳ－ROM１８の書き換えのみならず、重要なプログラムやデータが記録されている保護記憶領域、例えばＥＥＰROM１９、ハードディスク１６１内の特定記憶領域等の書き換えに対しても適用することができる。この様子を図７に示す。

【００４３】コンピュータウィルスが保護記憶領域の書き換えに必要な一連の処理手順を開始すると、その特定の手順で行われるハードウェアへのアクセスに応答して

前述のＳＭＩなどのハードウェア割り込み信号が発生され、これによって割り込みハンドラが起動される。割り込みハンドラは、プログラム認証を行い、不正な書き換えであればそれを阻止する処理を実行する。

【００４４】以上説明したように、本実施形態においては、ＲＯＭ書き換え用ハードウェアへの特定アクセスにより専用割り込みを発生させる仕組みを用いることにより、セキュリティ制御を適正な時点で実行させることができ、十分にセキュリティーレベルの高いシステムを実現することが可能となる。なお、ＳＭＩに限らず、他のハードウェア割り込みを利用し、ＯＳ上で動作するユーティリティなどを割り込みハンドラとして起動させるようにしてもよい。

【００４５】また、本発明は、上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【００４６】

【発明の効果】以上説明したように、本発明によれば、ソフトウェアによる不揮発性記憶装置の不正な書き換えを阻止できるようになり、十分にセキュリティーレベルを確保することが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンピュータシステムの構成を示すブロック図。

【図２】同実施形態のシステムで使用されるフラッシュＲＯＭ書き換え制御処理の手順を示すフローチャート。

【図３】同実施形態のシステムで使用されるフラッシュＲＯＭ書き換え制御処理の第２の手順を示すフローチャート。

【図４】同実施形態のシステムで使用されるフラッシュＲＯＭ書き換え制御処理の第２の手順を示すフローチャート。

【図５】同実施形態のシステムで使用されるＰＯＳＴ処理の手順を示すフローチャート。

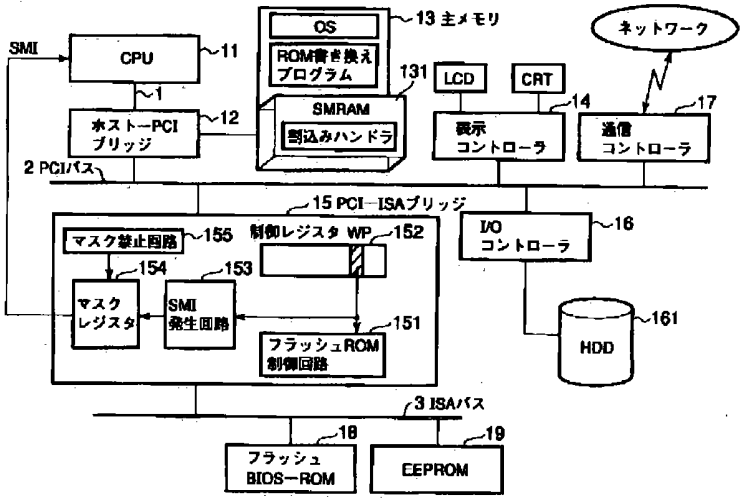
【図６】同実施形態のシステムで使用される割り込みハンドラ起動処理の他の例を示す図。

【図７】同実施形態のシステムで使用される割り込みハンドラの機能拡張の一例を説明するための図。

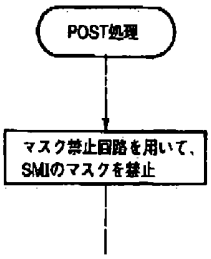
【符号の説明】

１１…ＣＰＵ
１２…ホスト－ＰＣＩブリッジ
１３…主メモリ
１５…ＰＣＩ－ＩＳＡブリッジ
１６…Ｉ／Ｏコントローラ
１７…通信コントローラ
１８…フラッシュＢＩＯＳ－ＲＯＭ
１９…ＥＥＰＲＯＭ
１３１…ＳＭＲＡＭ
１５１…フラッシュＲＯＭ制御回路
１５２…制御レジスタ
１５３…ＳＭＩ発生回路
１５４…マスクレジスタ
１５５…マスク禁止回路

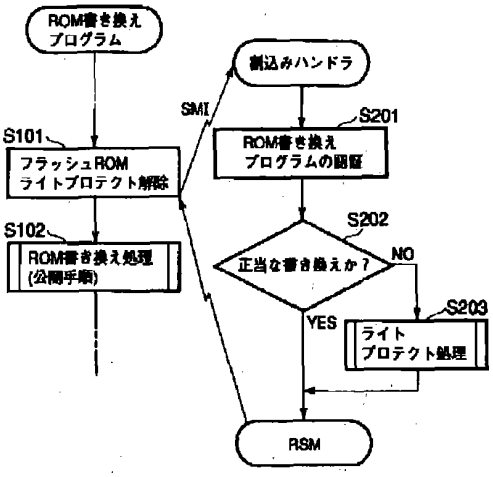
【図１】



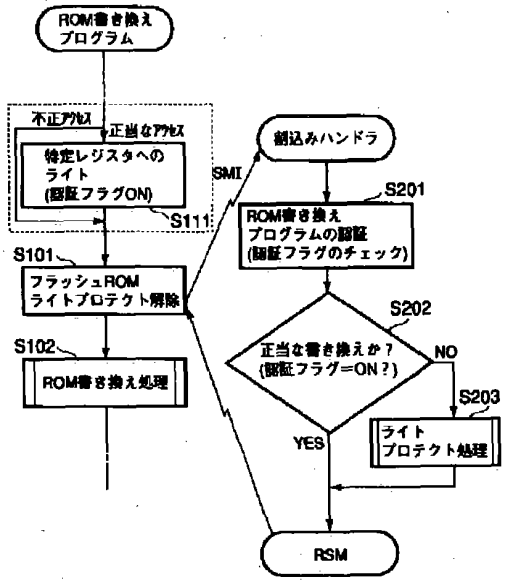
【図５】



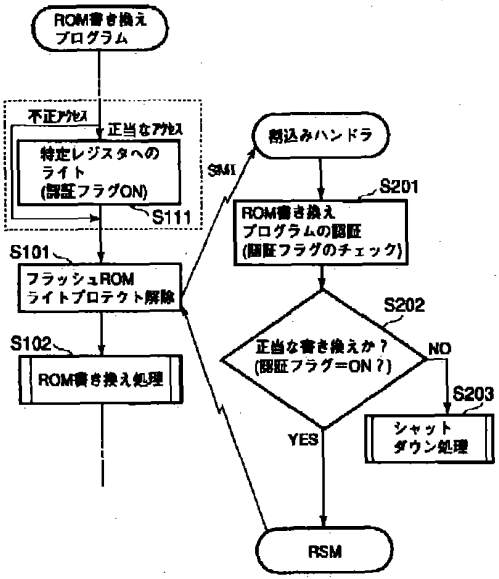
【図２】


ROM書き換え
プログラム
割込みハンドラ
SMI
S201
ROM書き換え
プログラムの認証
S101
フラッシュROM
ライトプロテクト解除
S202
正当な書き換えか？
NO
S102
ROM書き換え処理
(公開手順)
YES
S203
ライト
プロテクト処理
RSM

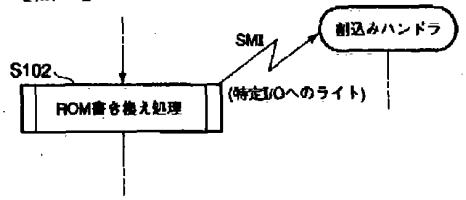
【図３】


ROM書き換え
プログラム
不正アクセス
正当なアクセス
特定レジスタへの
ライト
(認証フラグON)
S111
割込みハンドラ
SMI
S201
ROM書き換え
プログラムの認証
(認証フラグのチェック)
S101
フラッシュROM
ライトプロテクト解除
S202
正当な書き換えか？
(認証フラグ=ON？)
NO
S102
ROM書き換え処理
YES
S203
ライト
プロテクト処理
RSM

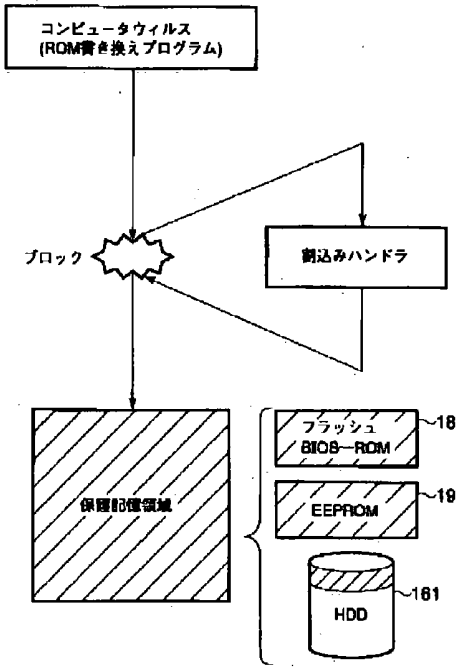
【図４】


ROM書き換え
プログラム
不正アクセス
正当なアクセス
特定レジスタへの
ライト
(認証フラグON)
S111
割込みハンドラ
SMI
S201
ROM書き換え
プログラムの認証
(認証フラグのチェック)
S101
フラッシュROM
ライトプロテクト解除
S202
正当な書き換えか？
(認証フラグ=ON？)
NO
S102
ROM書き換え処理
S203
シャット
ダウン処理
YES
RSM

【図６】


SMI
割込みハンドラ
S102
ROM書き換え処理
(特定I/Oへのライト)

【図７】


コンピュータウィルス
(ROM書き換えプログラム)
ブロック
割込みハンドラ
保護記憶領域
フラッシュ
BIOS—ROM
18
EEPROM
19
HDD
161